

NAVSUBSCOLINST 2201.1B
N5
4 May 1999

NAVSUBSCOL INSTRUCTION 2201.1B

Subj: PROCEDURES FOR INTERNAL DISTRIBUTION AND CONTROL OF
COMMUNICATIONS SECURITY MATERIAL SYSTEM (CMS)
PUBLICATIONS AND DEVICES

Ref: (a) CMS-1A

Encl: (1) Class CMS User Acknowledgement form (A)
(2) Watch-to-watch Inventory Sheet

1. Purpose. To promulgate instructions for CMS user personnel concerning handling, accountability, destruction, and disposition of COMSEC within the command.

2. Cancellation. NAVSUBSCOLINST 2201.1A. This instruction has been revised extensively and should be read in its entirety.

3. Background. The CMS provides for security of certain highly sensitive classified material and related publications, most of which require positive control and accountability throughout the useful lifetime of the material. Each command with a CMS account is required to designate a CMS Custodian and Alternate Custodians who will be responsible for proper administration of the command's account. Reference (a) contains detailed instructions for issuing, accounting, handling, safeguarding and destroying or otherwise disposing of CMS materials. These procedures are promulgated for internal distribution and control of CMS in compliance with reference (a).

4. Responsibilities

a. Commanding Officer. In accordance with reference (a), the Commanding Officer is ultimately responsible for properly administering the command's CMS account and ensuring compliance with established policy and procedures.

b. CMS Custodian. An individual designated in writing by the Commanding Officer to manage the material issued to the CMS account. He/She is the Commanding Officer's primary advisor on matters concerning security and handling of COMSEC material and associated records and reports.

c. Alternate Custodian(s). The CMS Alternate Custodian(s) is/are designated in writing by the Commanding Officer to assist the CMS Custodian in the performance of his/her duties and assume the duties of the CMS Custodian in his/her absence. Alternate Custodian(s) share equally with the CMS Custodian for responsibility of proper management and administration of the CMS account.

d. CMS User. An individual designated in writing by the Commanding Officer who, regardless of whether or not they have signed personally for COMSEC material, requires COMSEC material to accomplish an assigned duty and has obtained the material from a Custodian or another User on local custody. CMS Users must comply with procedures for handling and accountability of CMS placed in their charge.

5. Procedures

a. Access. Access to classified CMS must be restricted to properly cleared individuals whose official duties require access to COMSEC material. The fact that an individual has a security clearance and/or holds a certain rank or position does not, in itself, entitle an individual access to COMSEC material. Access to classified as well as unclassified COMSEC material requires a valid need-to-know. All personnel having access to COMSEC keying material must be authorized in writing by the Commanding Officer. An individual letter or an access list may be used for authorization.

(1) If an individual letter is used, the letter remains in effect until the status for the individual changes.

(2) If an access list is used, it must be updated whenever the status of an individual changes, or at least annually.

b. Student Requiring Access. Students currently attached to Naval Submarine School who require access to COMSEC material must review reference (a) and NAVSUBSCOLINST 2201.1 (series), then sign enclosure (1) of this instruction acknowledging responsibility for proper handling and safeguarding of COMSEC material.

(1) Enclosure (1) shall be kept in the class folder until class graduation. Once the class has graduated the enclosure will be forwarded to the CMS Custodian and retained for 90 days.

c. Two-Person Integrity (TPI) Requirements. TPI is a system of handling and storing designed to prevent single-person access to certain COMSEC material.

(1) TPI handling requires that at least two persons, authorized access to COMSEC keying material, be in constant view of each other and the COMSEC material requiring TPI whenever that material is accessed and handled. Each individual must be capable of detecting incorrect or unauthorized security procedures with respect to the task being performed.

(2) TPI storage requires the use of two approved combination locks (each with a different combination) with no one person authorized access to both combinations.

d. COMSEC Material requiring TPI. TPI must be applied to the following COMSEC material from time of receipt through issue to destruction.

(1) ALL TOP SECRET paper keying material marked or designated CRYPTO.

(2) Fill Devices (FDs) containing unencrypted TOP SECRET key.

(3) Equipment containing TOP SECRET key that allows for key extraction.

e. COMSEC material completely exempt from TPI. TPI is not required for COMSEC keying material marked SECRET, CONFIDENTIAL, or UNCLASSIFIED, regardless of CRYPTO markings.

f. Access to and protection of safe combinations. Each lock must have a combination composed of randomly selected numbers based on constraints of the manufacturer. The combination must not deliberately duplicate a combination selected for another lock within the command and must not be composed of successive numbers, numbers in a systematic

sequence, or predictable sequences (e.g., birthdates, social security numbers, and phone numbers).

(1) Custodian combinations shall be known only to the Custodian and Alternate Custodians. No one person will be allowed access to, or knowledge of both combinations to any one TPI container.

(2) Safe combination envelopes for the CMS spaces and safes will be maintained by the Physical Security Department and access controlled by the Physical Security Department or the Officer Of the Day for emergency access.

g. Storage. Storage spaces for COMSEC material shall provide the best possible protection against unauthorized personnel access and material damage or deterioration. They shall be secured when not under direct supervision of appropriately cleared and authorized personnel. Storage containers for COMSEC material outside the CMS vault shall be approved by the CMS Custodian in accordance with requirements outlined in reference (a).

h. Required CMS User files. Each CMS User account will establish and maintain a CMS User file. The CMS User file will contain a minimum of the following:

(1) All effective, signed local custody documents (i.e., SF 153 or locally prepared equivalent form) reflecting the issue of COMSEC material charged to the User.

(2) Effective watch-to-watch inventory.

(3) A copy of the effective NAVSUBSCOLINST 2201.1 (series).

(4) A copy of the effective NAVSUBSCOLNOTE 2200.

(5) A copy of the signed CMS User acknowledgment form for all members of the local User account.

i. Destruction. Effective and superseded keying material is extremely sensitive, and if compromised, potentially exposes to compromise all of the information encrypted by it. For this reason, keying material (other than defective or faulty key) must be destroyed as soon as

possible after it has been superseded or has otherwise served its intended purpose. Due to the COMSEC material holdings charged to Naval Submarine School, destruction of COMSEC material other than training/maintenance keying material (i.e. operational keying material, equipment, maintenance manuals, operating instructions, and general doctrinal publications) will be performed by the CMS Custodian or Alternate. Destruction of regularly or irregularly superseded training/maintenance keying material segments will be performed by the CMS Custodian, Alternate, or User when it becomes physically unserviceable. If the entire edition of the training/maintenance material has been superseded return the effected material and all destruction reports for the material to the CMS Custodian for complete destruction.

(1) Destruction Personnel. COMSEC material that is authorized for destruction must always be destroyed by two cleared and authorized personnel in accordance with the following:

(a) Unissued (i.e., retained in the vault or safe of the Custodian) superseded COMSEC material must be destroyed by custodian personnel, or by the Custodian or Alternate and a properly cleared witness.

(b) Issued (i.e., to a LH/User for use) superseded COMSEC material must be destroyed by any two properly cleared and authorized personnel.

(2) Routine Destruction of Keying Material
Destruction will be completed immediately after use when more than one copy of key setting is available, or as soon as the end of the crypto period and always within 12 hours after the end of the crypto period. Exceptions to the 12-hour destruction standard will be in accordance with reference (a), Article 450.

j. Inventories. COMSEC publications and keying materials will be stored in their assigned COMSEC material safe when not in use. All COMSEC material held by a CMS User shall be inventoried each day the safe is opened, or area is manned, using the following guidelines:

(1) All material issued by the CMS Custodian shall be listed and accounted for using enclosure (2). The person

conducting the inventory and page check(s) shall sign the inventory form. New material received by the users shall be added to the inventory listing. New material shall indicate the date material was received. Material destroyed or returned to the CMS Custodian shall be lined out from the date the material was destroyed or returned. Deletions shall be initialed and the date and disposition of the material noted on the listing.

(2) Accountability and custody shall be established by the following criteria:

(a) COMSEC material will be listed by short title, edition, register number, accounting number and quantity.

(b) All COMSEC equipment, including Controlled Cryptographic Item (CCI) equipment, shall be listed by short title and quantity.

(3) Any discrepancies identified will be reported **immediately** to the CMS Custodian.

(4) Superseded inventory listings shall be turned in to the CMS Custodian, who will retain them for 30 days.

k. Page checks. Page checks shall be conducted on initial issue and on all items indicated by an asterisk on the inventory sheet. Page checks will be conducted on all unsealed keying material. Unsealed keying material includes: each key tape segment unintentionally removed, segments that cannot be destroyed immediately after use, and last copy of multiple-copy keys. Destruction reports will be utilized to establish continuity and complete accountability of code books or key tape canister segments. Page checks will be conducted on KAMs and KAOs used by students upon issue and prior to graduation of the class.

l. Amendments. Amendments or corrections to CMS issued for entry will include a copy of Figure 7-4 from the CMS 1A as a guide. The first person will enter the amendment in accordance with reference (a) as soon as possible after receipt. A second person will verify proper amendment entry.

m. Damaged, Worn or Mutilated Publications. Damaged,

worn or mutilated publications will be returned to the CMS Custodian for replacement. The Custodian will handle this material in accordance with reference (a).

n. Reproduction. Extracts and/or copies of COMSEC material will not be made unless properly authorized in accordance with reference (a). When authorized, extracts

and/or copies will be made only with the consent and control of the CMS Custodian.

o. COMSEC Material Incidents. Any actual or suspected loss or compromise of COMSEC material shall be reported immediately to the CMS Custodian. The CMS Custodian shall then notify the Commanding Officer and take the actions required by reference (a).

p. Removal of COMSEC material. Under no circumstances will COMSEC material be removed from the command by anyone other than the CMS Custodian or Alternate, and then only with the Commanding Officer's permission.

q. Returning COMSEC material. CMS Users shall keep the CMS Custodian informed of their impending TAD, leave, or PCS transfer and will return all CMS material prior to their departure.

r. Emergency Action Plan. The CMS Custodian shall ensure that a detailed Emergency Action Plan for all COMSEC material is prepared and updated periodically. All CMS Users will thoroughly familiarize themselves with the provisions set forth in the Emergency Action Plan.

6. Action. The CMS Custodian shall ensure that CMS material administrative personnel understand their CMS responsibilities and that they are sufficiently trained to carry out their duties. In executing this responsibility, the CMS Custodian shall:

a. Monitor the overall internal security, accountability control and destruction of COMSEC material, and provide oral and written guidance.

b. On a periodic basis, review all responsible user inventories to ensure they are prepared and executed

properly. Initial the inventory to document this review.

c. Ensure that a detailed and updated Emergency Action Plan is read at least annually, and exercised by all personnel at each station where COMSEC material stored or handled at least semi-annually.

d. Monitor the proper inventory of COMSEC material held by Users.

e. Maintain a record of all CMS related training held, both formal and informal.

K. B. LEAHY

DISTRIBUTION:
CD-ROM

I CERTIFY THAT I HAVE PERSONALLY SIGHTED AND INVENTORIED EACH OF THE ABOVE LISTED MATERIALS AND PAGE CHECKED THOSE INDICATED BY AN ASTERISK (*). BY MY SIGNATURE I ACKNOWLEDGE RESPONSIBILITY FOR MAINTAINING SECURITY OF ALL THE

Enclosure (1)

ACCOUNT 179105

MONTH_

PAGE_

OF

[illegible]

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

I CERTIFY THAT I HAVE PERSONALLY SIGHTED AND INVENTORIED EACH OF THE ABOVE LISTED MATERIALS AND PAGE CHECKED THOSE INDICATED BY AN ASTERISK (*). BY MY SIGNATURE I ACKNOWLEDGE RESPONSIBILITY FOR MAINTAINING SECURITY OF ALL THE MATERIAL LISTED. I WILL REPORT ANY DISCREPANCIES TO PROPER AUTHORITY THROUGH MY CHAIN OF COMMAND.

CMS RESPONSIBILITY ACKNOWLEDGMENT FORM

Class Number _____

From: _____
To: Naval Submarine School CMS Custodian

Subj: **CMS RESPONSIBILITY ACKNOWLEDGMENT**

Ref: (a) CMS 1A
(b) NAVSUBSCOLINST 2201.1

1. I hereby acknowledge that I have read and understand references (a) and (b).
2. I assume full responsibility for the proper handling, storage, inventorying, accounting, and disposition of the COMSEC material held in my custody and/or used by me.
3. I have been provided a copy of references (a) and (b) for review. If at any time I am in doubt as to the proper handling of COMSEC material that I am responsible for, I will immediately contact the CMS Custodian and request advise.
4. Before extended departure from the command, (i.e., permanent transfer, or leave/TAD/TDY in excess of 30 days) I will report to the CMS Custodian and be relieved of responsibility for all COMSEC material that I have signed for.

Course Number _____ Class Number _____

Name (print)	Signature	Date
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

Enclosure (2)

